Internet Censorship: Freedom vs Security

Rohan Khanna[1], Vikram Dhingra[2], Kavita Choudhary[3]

Student B.Tech CSE[1], Student B.Tech CSE[2], Asst. Professor[3]

ITM University, Gurgaon, India

Abstract—The internet as we know it today has transformed itself from the world's only nuclear strike resistant communications network, into the world's only true medium of free, uncensored speech. It was thought that the internet would improve and increase global human development through the promotion and easy transmission of ideas and thoughts. However, in these past few years, we have noticed unexpected developments in this field. Various corporate and government entities are trying to monitor, censor and altogether control this once free internet. With entities such as SOPA, PIPA, TPP, Patriot act, Telecommunications act and India's very own ICMS challenging and threatening the very notion of human freedom, it is important to educate people regarding the very force that is trying to corrupt this publically owned network. In this paper we will be covering the security aspect of Internet domain. As we all know, the internet was invented in The USA by the name of ARPANET, and was originally intended to be used as a nuclear strike resistant network. It consisted of only a handful of nodes, and was not even used to connect computers together at its first inception. The USA has been the pioneer of internet and wireless communications since then, and has held on to all the powers that hold the internet together since then. They own all 14 of the DNS servers throughout the world, without which the internet cannot translate human readable addresses into computer understandable addresses. The USA has shut down many websites that were hosted on the domains of other countries. Thepiratebay and wikileaks are prime examples, and many more are being discussed as we speak. With the reducing cost of technology and easier access, The USA has already implemented a nationwide monitoring system called PRISM, which monitors and records all real and digital movement in the country.

***Keywords*— e-Censorship, Internet Governance, DNS Injection, SOPA etc.**

Introduction

The internet as we know it today is the world's largest platform for free speech and expression. It is a highly interconnected mesh of millions of computers connected together throughout the world to form what we call the World Wide Web. It keeps billions of people connected to each other, and life today would be very different without it. The world at our fingertips, as some would call it, the internet brings together people of separate nationalities, speaking different languages, and bridges the cultural divide unlike nothing else in the world, and has stayed strong through the years until today. The internet has helped destroy cultural stereotypes, and has provided an outlet for individuals to voice their opinions against unfair and unlawful ideology and practices. The speed and flexibility of internet data routing protocols is due to the network being designed with failure in mind. The network continues to function even if a large part of it is taken offline. This is due to the decentralized nature of the internet. That is, it is independent of any central entity which controls the functioning of the internet. However true this may be, various forces of political and corporate agenda are creeping closer and closer to their ultimate goal of corrupting the very fabric that keeps the internet free and open for all its participants. These forces are mainly of American origin namely SOPA (stop online piracy act), PIPA (Protect Intellectual property act), The Patriot act and The Telecommunications act. Also, India's very own ICMS (Indian Central monitoring system) [4] has also recently been seen in the news. The implications of large scale monitoring are huge. The technical difficulties behind monitoring of internet communications and its censorship are relatively similar, so any act of unlawful monitoring also poses a potential threat of censorship also. China and North Korea are prime examples of this phenomenon. India is obviously not too far behind in this field. If uneducated regarding the consequences, our citizens might become victim to permanent large scale wire-tapping and we might possibly become another China.

The first step of this journey will question the motives of the forces behind such practices, and throw light on how internet censorship affects daily life on a global scale. The second step of the journey is a hunt for alternative technologies and

practices to help safeguard ourselves from the evils of censorship. We might go deeper into the internet to locations called the dark net; i.e. a part of the internet that is securely cut-off from the rest of the internet(called the surface-net) and is kept secret from prying eyes, by means of strong , open-source cryptographic security and alternative routing mechanisms to achieve true online anonymity.

Literature Survey

Bothma et. al. discussed that censorship is no longer limited to printed media and videos [1]. Its impact is felt much more strongly with regard to Internet related resources of information and communication such as access to websites, email and social networking tools which is further enhanced by ubiquitous access through mobile phones and tablets. Some ISPs and governments use DNS injection [2] to block access to "unwanted" websites. The censorship tools inspect DNS queries near the ISP's boundary routers for sensitive domain keywords and inject forged DNS responses, blocking the users from accessing censored sites, such as twitter and facebook. Unfortunately this causes collateral damage, affecting communication beyond the censored networks when outside DNS traffic traverses censored links. Xueyang et. al. explored where Intrusion Detection System (IDS) devices of the Great Firewall of China (GFC) are placed for keyword filtering at router level [3]. Knowing where IDSes are attached to better understand the infrastructure of the firewall, gain more knowledge about its behavior and find vantage point for future circumvention techniques.

Bridging the gap between Early Internet & modern Internet

In 1993, *Time Magazine* article quoted computer scientist John Gilmore, one of the founders of the Electronic Frontier Foundation, saying "The internet interprets censorship as damage and routes around it". We might also wish to look at the fundamental property of the internet and confirm this statement by ourselves. The internet was designed as the world's largest mesh network, designed to provide connectivity to data by ensuring that data packets are capable of choosing their path of least resistance to reach their destination. If any routes are blocked, or taken offline, the network displays a unique form of "Intelligence" by effectively re-routing the data through an alternative route. Technical routing algorithms such as TTL and QoS are capable of doing so effectively, making censorship just an inefficient routing nuisance [5]. However, in the past few years, it has become obvious that censorship is now being driven by the full force of the law, and will be possibly used along with many such flimsy excuses such as "National security", "Piracy prevention" and even "Cleaning up the internet". As such, there exist 2 types of Censorship: Technical and Non-Technical censorship

Technical censorship is an implementation of software and code to track and censor the users of internet services by means of many techniques such as IP Filtering, DNS Filtering and redirection, URL Filtering, Packet Filtering, etc. There is no legal backing behind the act of technical censorship. These techniques may be voluntarily employed by network administrators of educational and corporate institutions, and might also be implemented by countries practicing pervasive censorship such as China, Saudi Arabia, North Korea, Iran and many others.

Non-technical censorship is the use and abuse of legal power to pass legislation to discourage and suppress the right to free speech under the threat of prosecution, monetary fines and even imprisonment. It is usually used in conjunction with technical censorship, although it is not 100% necessary to do so.

Currently, the most popular method of online censorship is the use of DNS redirection. The DNS or Domain Name System is a collection of 14 worldwide servers that store information regarding the IP addresses of the locations of websites, indexed by their name. To access anything on the internet, the data must be stored on a server, and that server must be connected to the internet, with a dedicated IP address. To access this server, one must know its IP address, or the IP address must be registered in the DNS table, which is owned by the American organization ICANN. The DNS is needed for the internet to work, because, one cannot possibly remember the IP address of all websites

that one uses, and still keep updating this list when there is a change in server locations. One needs a human readable address to network address translator, whose need is fulfilled by such a DNS. As long as a single entity owns and controls the DNS, censorship of websites is going to be technically very easy. A few solutions to this problem have risen to the challenge. They are in theory, alternative DNS systems, and need to be configured by the browser to be used, instead of the ICANN servers. They may be hosted on private servers, or may be completely decentralized, running off the resources of the computers of the users. A few examples include OpenNIC, Open Root Server Network, Public-root, and more interestingly, a digital currency inspired DNS System called Namecoin. These systems are independent of the ICANN, and there are no legal restrictions currently regarding their usage. The decentralization of most online services as we move towards the future is going to be a key factor in this global scale conflict of interest, with many new innovations to come and change the way we communicate for all time.

Impact on Human Development

The Internet has been a true gift to mankind. Using the internet we can communicate, share, learn and teach everything from the fields of science and art without any boundaries and limitations [2] [3]. The internet is a crucial piece of technology, which has successfully integrated itself with human existence, and helped shorten gaps and break existing barriers to help people come closer. Without the internet, we are crippled. A very recent example of this was when Egyptian authorities took down the internet infrastructure during the 2011 riots. When Egyptian authorities demanded telecommunication services to shutdown, there was a total internet blackout. What happened in Egypt necessitates the need to understand the entire Internet ecosystem, when it comes to considering the question of a censorship-free Internet. Both children as well as adults use the internet to learn and understand many critical problems which they are not able to analyze in day to day life just by themselves. The internet exposes us to good quality information which results in cognitive development of the mind and increases awareness of our surroundings. The role of the internet is heightened when it plays a part in debunking misinformation which may be spread by political or unsocial elements to promote their own ideology. Being the fastest communication medium in the world, the internet has phenomenal applications in the fields of not just communication, but also that of information archiving and convenient access to this vast archive.

The Internet has undoubtedly played a key role in human social development. Websites like Facebook, Reddit and Twitter etc help us connect with other people with whom we possibly could not have real human interaction. The internet besides being an educational tool also provides access to quality entertainment, often without any cost depending on the sources, considering that lack of quality entertainment affects society adversely in its own way. The internet is always alive with debate and conversation with its favorite topics being an infinite spectrum of new ideas in various fields such as politics and religion. With the world's entire scientific community having a strong online presence, the internet is cheekily described as "The place where religion comes to die". It lives up to this description remarkably. Due to the participants being mostly open minded youth and scientifically literate individuals, the life of the community is maintained by the seemingly infinite turns that conversations can take, all without putting any geographical, societal or monetary pressures upon the participants involved.

One of the rare observable negative impacts on human development is that real human interaction and relationships are slowly being replaced by virtual, online ones.

Future Possibilities & Conclusion

Many websites have been shutdown under the guise of internet security, and to safeguard from digital piracy. Thepiratebay and Wikileaks were a few such examples of the first websites to be blocked from the public by many developed countries. The United States of America were the first to prevent their public from accessing these websites and stated that these two websites posed a threat to national security as well as to their

economy, the notion of which is not yet backed with any measurable proof.

Thepiratebay, commonly known as TPB, was founded in Sweden by Peter Sunde, Gottfrid Svartholm and Fredrik Neij in 2003. TPB fulfilled a need at its time by providing a platform for peer to peer file sharing using the Bittorrent protocol. Bittorrent changes the way content is distributed online by replacing the client server model with a model where each downloader also becomes an uploader of the data to other "peers" that may need this data. This innovative protocol effectively reduces the content distribution load to be borne by the distributor. TPB has been questioned and banned numerous times in the past. At some point in time TPB has been banned in Belgium, Denmark, Finland, Germany, India, China and Sweden. In 2006, many American record and media companies collectively filed a case against TPB, charging it with multiple counts of Copyright Infringement, which has cost them $3.4 million. The Case's verdict was out in 2008 and TPB was found guilty. TPB was shutdown, but TPB challenged the verdict, but nothing fruitful resulted out of it. They were sentenced to a year of imprisonment and fined $ 2, 700, 00. But in 2013 TPB was back again. TPB has just recently completed 10 years of its life which is a milestone for Internet Freedom and censorship-free Internet [5]. The latest technologies in secure communication are mainly Tor and Freenet. These tools, along with countless other lesser known technologies are effective against online monitoring and censorship. The innovation and technical competence employed by the inventors of these technologies is the reason that these technologies are able to promise air-tight privacy. Its anonymity has made it popular among numerous users who are willing to sacrifice Internet speed for privacy-enhanced web access. But it doesn't overcome the threat on government/corporate control of the Internet. The real challenge is to create censorship-free Internet technologies which would sustain it even when other entities are vying for control over it. In December this year, some governments of the world, along with a select few corporations are having a closed–door meeting called the Trans Pacific Pact over how the control would be implemented to further their own agenda by putting legal as well as technical barriers over the once free internet. As described by the UN Universal Declaration of Human Rights, the right to free, uncensored speech is a basic human right, as is the right to privacy. The Internet is the bane of all human development and our collective future. Putting restrictions on it will only result in large scale conflict and revolt which is detrimental to the well-being of both parties. If any single entity happens to take control of the Internet then the following is most likely to happen:

1. They will be able to observe, modify, block, delay, replay, and modify the traffic according to their wishes.
2. No transparency would exist as all information would be censored, or only misinformation would be disseminated. These entities will obviously only publish that information which will be in their favor.
3. They will have complete unrestricted access over the data stored and transmitted from all internet connected computers and smart-phones.
4. The new laws might legally enforce all cryptographic keys to have inbuilt flaws so that they would be remotely exploitable by these entities.

References

1. Bathma, Fourie and Bitso, Trends in transition from classical censorship to Internet Censorship.

2. Zion Virual Labs, The collateral damage of internet censorship by DNS Injection.

3. Xueyang Xu, Z Morley Mao and J Alex Halderman, Internet Censorship in China.

4.http://searchengineland.com/the-impact-of-the-internet-on-human-behavior-20921

5.http://www.internetsociety.org/articles/moving-toward-censorship-free-internet?gclid=CJ316pPx97gCFYJU4godXU8AEw